LEVERAGING ITIL/ITSM INTO NETWORK OPERATIONS

GRADUATE RESEARCH PROJECT

DAVID A. LAVINE SR., Major, USAF

AFIT/ICW/ENG/11-07

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

AFIT/ICW/ENG/11-07

Leveraging ITIL/ITSM into Network Operations

GRADUATE RESEARCH PROJECT

Presented to the Faculty

Department of Electrical and Computer Engineering

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Cyber Warfare

DAVID A. LAVINE SR.

Major, USAF

June 2011

AFIT/ICW/ENG/11-07

Leveraging ITIL/ITSM into Network Operations

DAVID A. LAVINE SR.
Major, USAF

Approved:

/signed/	1 Jun 2011
Jonathan A. Butts, Capt, PhD (Chairman)	date
/signed/	1 Jun 2011
Richard A. Raines, PhD (Member)	date

Abstract

Air Force Network Operations (AFNetOps) controls the AF portion of the Global Information Grid (GIG). In order to do this efficiently, the USAF had to change the way it was operating and go away from Centralized Control, Decentralized Execution towards Centralized Control, Centralized Execution. This was done largely in part because the USAF was struggling in protection of critical information and the networks interconnecting all of our installations. In the Late 80's the United Kingdom created Information Technology Infrastructure Library (ITIL) whose purpose is to provide a practical no-nonsense framework for identifying, planning, delivering and supporting IT services for a business. Over the years, ITIL has become the defacto standard for IT Service Management. In consolidating our Network Operations and Security Center operations, the USAF decided to take steps towards incorporating this standard. This research discovered how well ITSM was ingrained into our AFNetOps posture and the collaborative efforts to standardize change management for the benefit of the Air Force. If indeed the USAF is to become another ITIL success story, it resides with the IT Service Management framework of guiding our NetOps.

Acknowledgements

First and foremost, I want give thanks to God for his grace and mercy because all things are possible through him. Secondly, I would like to thank my family for their love and support. A special thanks to Dr. Mills, Dr. Butts and Dr. Raines for their guidance over this year and Dr. Mullins for opening my eyes to another level of Cyber.

Lastly, I would like thank Maj Gen (ret) Maluda, Col (ret) Clapp, Col (ret) Hunninghake, Col (ret) Heinke, the I-NOSC Tiger Team, Commanders from the 67th NWW, 690th NSG, 33rd NWS, 299th NOSS, 561st NOS, 83rd NOS and all the other outstanding professionals that contributed to this research.

DAVID A. LAVINE SR.

Table of Contents

List of Figures

Leveraging ITIL/ITSM into Network Operations

I. Introduction

1.1 Background

A decade ago, the United States Air Force realized that the current method for managing the information technology (IT) infrastructure was not sustainable. To meet the demanding needs and respond to technological advances, the Air Force had to instigate a cultural shift and make an unpopular decision that would have consequences for years to come. At the time, each Major Command (MAJCOM) owned and operated a network operations and security center (NOSC), which oversaw all network operations within the respective MAJCOM. In short, each NOSC was the convergence point for all communications within that command. A need for increased interoperability and reliance across the Air Force portion of the global information grid (GIG) drove this commission. The Air Force network operations (AFNetOps) strategic plan called for a "transformation of the GIG from a loose federation of MAJCOM centered components to an enterprise-centric network. Day-to-day Command and Control (C2) of the network had to be exercised by a single commander" [4]. As a result of the strategic plan, the NOSCs were directed to integrate and transformed into a centralized control, centralized execution posture (see Figure 1).

To implement this substantial undertaking, the Air Force assembled a team of experts to define the way forward. Overshadowed by constraints in the form of unforeseen political pressure, tight budgets and reluctance to change, the team produced a seemingly sound product. However, now that several years have passed, the decisions warrant investigation to determine what aspects were effective and what shortfalls need improvement. For example two I-NOSCs, each responsible for half of the Air Force portion of the GIG, maintaining the same level of service is a daunting, but not impossible task.

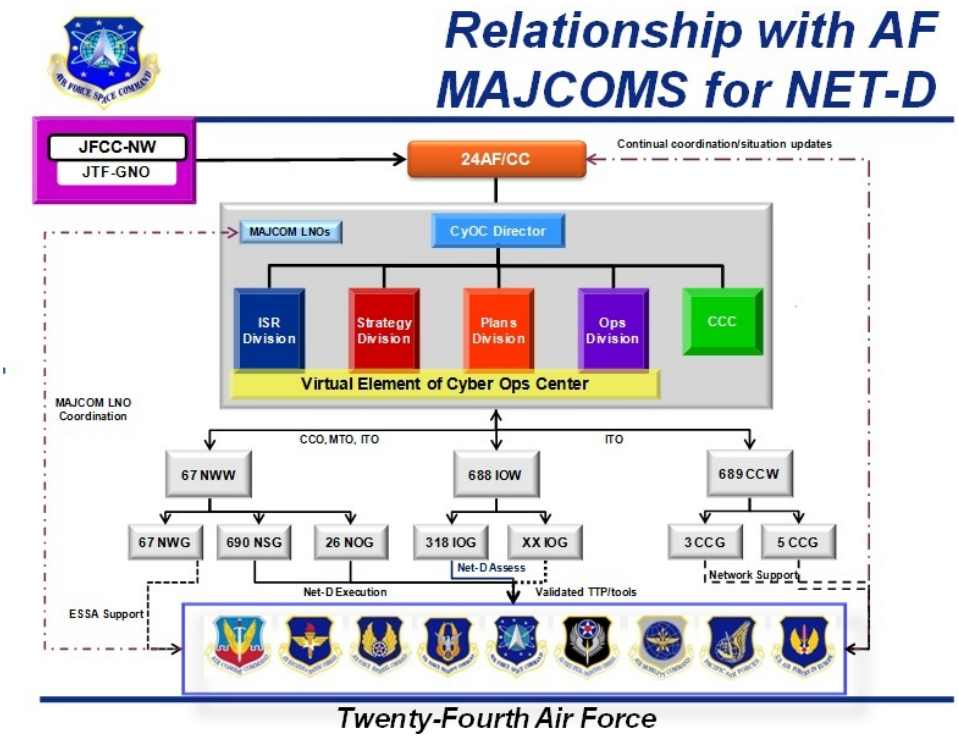

Figure 1: 24 AF Structure

1.2 Approach

Between 1989 and 1995, the United Kingdom (UK) created the Information Technology, Infrastructure Library (ITIL). Its purpose is to provide a practical no-nonsense framework for identifying, planning, delivering and supporting IT services for a business [5]. The primary benefits of applying ITIL principles are:

1. Improved availability, reliability, and security of mission critical IT services
2. Document and communicate roles and responsibilities in service provision
3. Optimized IT infrastructure providing for all business requirements
4. Permanently lowered total cost of IT ownership including service cost

This research performs an in-depth look at ITIL and examines if the Air Force has successfully incorporated the proven principles into the infrastructure that emerged from the transformation of AFNetOps. A key component with ITIL is that it advocates that IT services must be aligned to the needs of the business. It provides

guidance to organizations on how to use IT as a *tool* to facilitate business change, transformation and growth. Disney's CIO began adopting ITIL best practices in the mid 2000s and is now one of the true ITIL success stories. Indeed, Disney made an investment in the ITIL process; the return on that investment was increased revenue and maintained excellence [6].

To facilitate this research, several visits to the I-NOSCs and discussions with their leadership was performed. The interviews and site visits helped provide insight to the following two questions:

1. Have they incorporated ITIL principles within the AFNetOps construct?
2. Through examination of the three I-NOSCs with respect to the ITIL process, are there areas that need improvement?

1.3 Motivation

The network operations squadrons in the Air Force are charged with providing the services that enable a MAJCOM's command and control capabilities. Over the years, the complexity of this mission has increased, while at the same time the networks have been under constant attack. As the structure started transforming over the years, Air Force leadership began questioning the efficiency. According to Maj Gen Basla "Right now, we do not have the full suite of tools - automated tools we could use to help analyze all the data that's coming in and provide situational awareness, that common operational picture, that understanding of the battlespace that we want to" [7]. There are, no doubt, areas that would benefit from a process improvement program. One such historically proven program is the ITIL process. The analysis of network operations with respect to ITIL can help streamline how tasks are being accomplished and identify efficiencies for daily operations.

1.3.1 Purpose. Over the past five months, visits were arranged with organizations that function as fusion centers for network operations. The preponderance of this research focuses on the Air National Guard Network Operations Security

Squadron (299th NOSS), 561st NOS and 83rd NOS. However, the information gleaned from 624th Operations Center, 67th Network Warfare Wing, 690th Network Support Group, 33rd Network Warfare Squadron, 690th Network Support Squadron and the Air Education and Training Command (AETC) MAJCOM Communication Coordination Center contributed to the analysis.

The purpose of the research is to identify gaps in the management of Air Force IT services and recommend improvements. Specifically, this research analyzes success and/or failure of ITIL principles in current Air Force network operations. The research examines three of the primary ITIL principles and determines how the two primary I-NOSC squadrons (561st NOS and 83rd NOS) and the 299th NOSS incorporate the historically successful process improvement program.

1.3.2 Organization. The remaining research is organized as follows. Chapter 2 discusses the origin and principles of ITIL. Chapter 3 discusses IT process management for Air Force network operations squadrons. Chapter 4 examines incorporation of ITIL into the network operations squadrons. Chapter 5 provides recommendations and Chapter 6 concludes this research project.

II. Overview of the Information Technology Infrastructure Library

> "This is a perhaps the best way in getting best business value from IT means, of course, leveraging incoming information from users and customers about service levels, resolution time and accuracy, customer satisfaction, technical performance and bottlenecks and emerging trends generally. Service desks thus not only generate value by helping IT solve problems users have encountered, or delivering services users need, but also by collecting information that can be leveraged in different ways for different purposes, and making it available to the rest of IT in order to drive business value in those domains as well." [8]

This chapter provides an overview of the British government's Central Computer and Telecommunications Agency (CCTA) Information Technology Infrastructure LIbrary (ITIL) process [5]. The CCTA initially developed the ITIL process and later joined with several other companies, ultimately being absorbed into the Office of Government Commerce (OGC) in the United Kingdom (UK). As a result, the UK adopted ITIL as part of their mission for commercial activities savings and improved success in the delivery of programs and projects. However, they quickly realized that ITIL had other far-reaching applications, and a mass distribution to public sector organizations commenced. Indeed, public and private organizations now use ITIL as their foundation for information technology (IT) management and it is recognized around the world as the de facto standard for applying service-centric management [9].

2.1 Background

ITIL is an integrated, process-based set of best practices for managing IT services. The framework consists of a library of volumes that describe best practices for: service support and delivery; implementation of service management; information and communication technology infrastructure management; application management; security management; and the business perspective [10]. A case study accomplished in the UK found that customer service, customer satisfaction and operational performance improvement as the primary areas that the ITIL framework improves [11].

The ITIL process is continually evolving. The initial volumes have been subsequently reviewed and edited, relying on the contributions of experts within each discipline. Proposed modifications are reviewed by the ITIL advisory group to ensure quality assurance and adherence to a set of defined standards. Additionally, ITIL undergoes periodic revisions. The OGC is committed to refreshing the volumes in order to keep the guidance up-to-date, as ITIL remains the worldwide focal point of IT service management. When the initial revision was completed in 2005, it was tabbed ITILv2. In 2006, ITIL was again revised focusing on associated certifications and tabbed ITILv3. Finally, the core volumes were condensed from seven to five books in the ITILv3 edition.

2.2 ITIL Structure

ITILv3 consists of five core publications: (i) service strategy, (ii) service design, (iii) service transition, (iv) service operation and (v) continual service improvement (see Figure 2). Each publication is an individual volume intended to stand on its own, yet compliment the overall ITIL process. For purposes of this research, the analysis focuses on service transition, service operation and continual service improvement. These three publications focus primarily on user interaction with IT services and the effects performance has on end users. The service design and service strategy publications more aptly apply to corporate and program office levels (see Figure 2).

2.3 Service Transition

Service transition is the delivery of services to users. Although day-to-day operations are important, service transition focuses primarily on major changes to an organization. For example, a new business process may require additional services, or a new upgrade to an operating system may be implemented. The ability to to sufficiently handle the roll out and minimize impact to users is critical. The primary processes that support service transition include transition planning and support, ser-

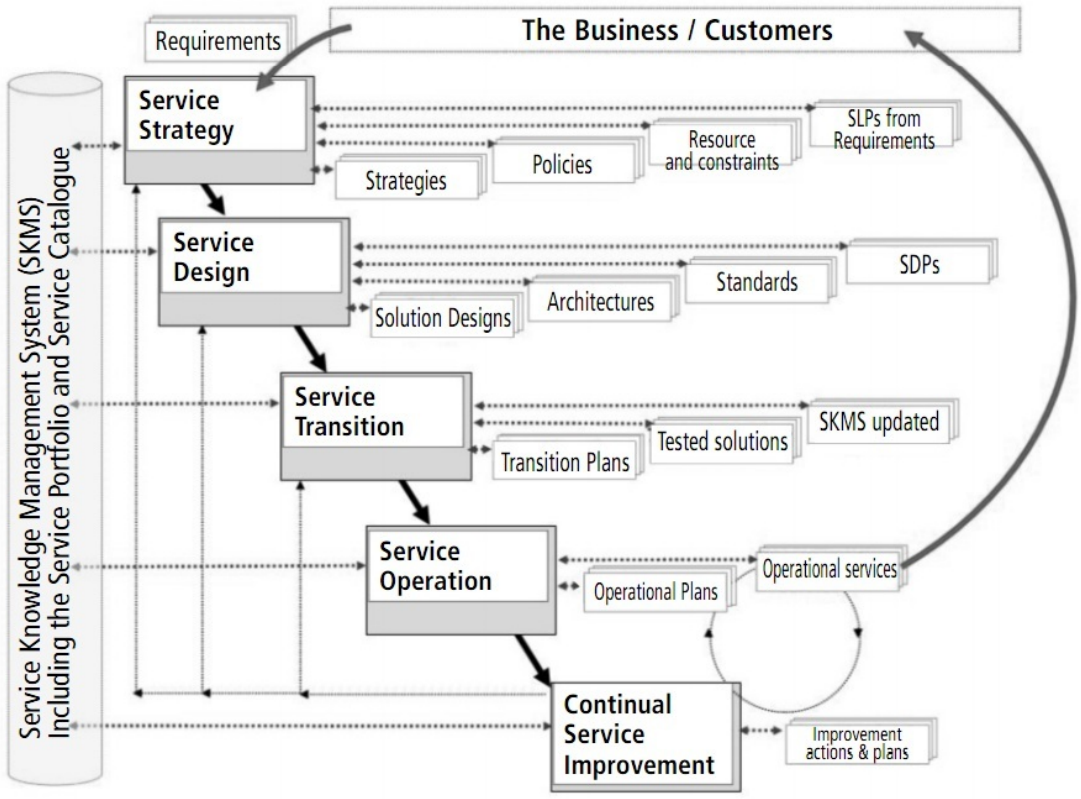

Figure 2: Service Lifestyle Stages

vice asset and configuration management, change management, release management, service validation and testing, evaluation, and knowledge management.

Transition Planning and Support . Transition planning and support ensures the relationship between service strategy and service design are incorporated into service operations. Transition planning and support also addresses contingency operations with respect to enterprise-wide services in the event of a failure.

Service Asset and Configuration Management . Service asset and configuration management provides detailed information of IT assets. It is important that equipment and resources are adequately accounted. This includes both physical accountability along with configuration settings for enterprise systems.

Change Management (CM). Change management has a distinctive role to ensure all facets of changes are appropriately planned for and impacts to end users are appropriately handled. Users traditionally resist change, particularly if the change impacts legacy operations or services. Change management helps manage expectations and ease transition by including users and documenting changes (e.g., user manuals). Figure 3 shows nominal interaction and responsibilities for various actors (i.e., business, service provider and supplier) according to the respective levels of change (i.e., strategic, tactical and operational).

Release Management. Release management focuses on version control. With multiple users leveraging myriad services, determining the most up-to-date version can be overwhelming. Appropriate measures to ensure accurate release and use of resources helps prevent confusion or incompatibility. Failure of proper release management can lead to devastating consequences that may not be noticed until many months after the initial problem occurs. At this point, it may be near impossible to recover from such a failure.

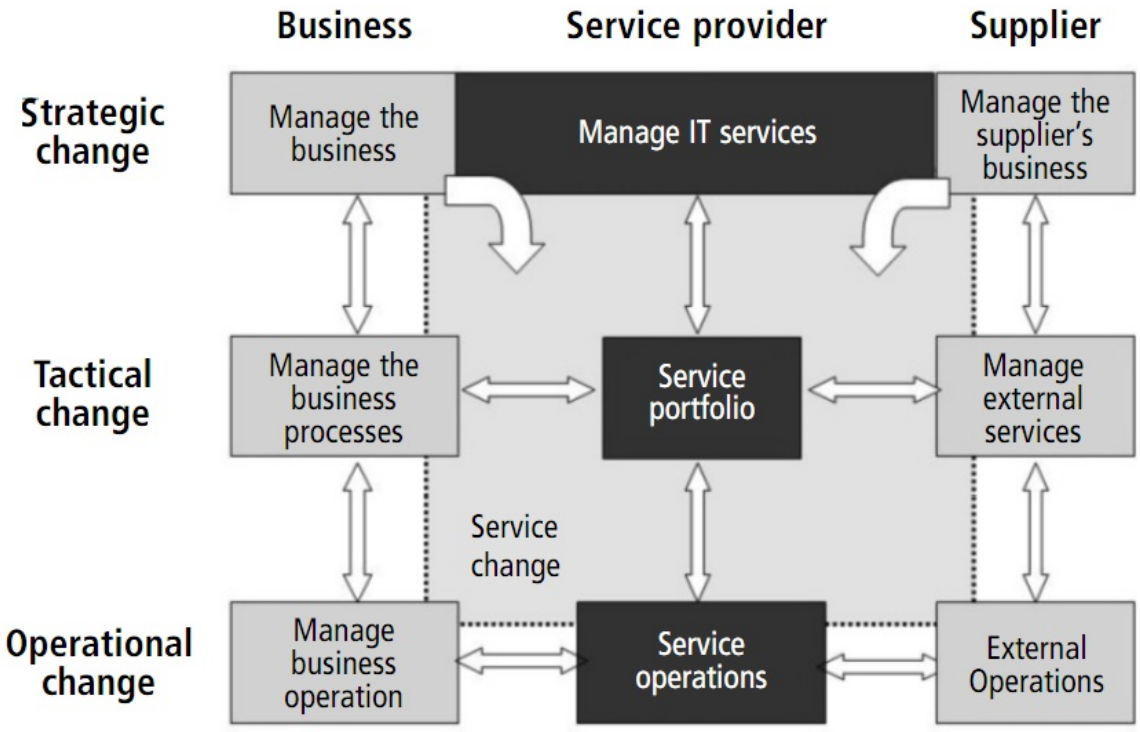

Figure 3: Change and Release Management for services

Service Validation and Testing. Service validation and testing is the component that ensures services meet the desired intent. Although typically considered an afterthought, service validation and testing should occur throughout the lifecycle and management of IT services.

Evaluation. This component evaluates the service transition inputs and validates the design and the transition approach. It primarily ensures that the IT services provided by the organization align with what the business needs to complete its desired goals.

Knowledge Management. Knowledge management is a multi-discipline aspect that leverages business process, management functions, and library and information sciences to ensure the right person, right knowledge and right time for management of IT functions for the organization. Without this component, an organization will suffer from personnel that are ill-equipped to do their jobs. Such actions can be

cancerous to an organization. Organizations can help facilitate the process through identification of appropriate knowledge, skills and abilities ahead of time. In this manner, employees have a full understanding of their roles and responsibilities before they perform their jobs.

2.4 Service Operation

Service operation delivers an agreed upon criteria for quality and class of service. These parameters are typically agreed upon and delivered according to a service level agreement between the service provider and the customer. It is important that apportionment of services is considered with respect to overall organization goals; if there is an inordinate amount of attention for one specific service, the overall effectiveness of the organization may suffer due to inadequate service. The primary processes for service operation are event management, incident management, request fulfillment and access management, and problem management.

Event Management. According to the recognized ITIL expert Alison Cartlidge (currently responsible for service management best practices across the UK and India), "an event is a change of state that has significance for the management of a configuration item or IT service" [12]. Events provide the user or system administrator with situational awareness for the current operating status of the system. Critical stops, unscheduled tasks, start and stops of processes are types of reportable events. Event management is dependent on monitoring for detecting and generating notifications. Additionally, monitoring provides insight into individual processes and can provide detailed information such as availability versus downtime. The responsiveness to an event may vary based on detection via an automated tool or a user monitoring the service.

Incident Management. Alison Cartlidge defines an incident as "an unplanned interruption to an IT service, or a reduction in the quality of an IT service. Failure of a configuration item that has not yet impacted service is also an incident" [12].

Accordingly, the incident management task restores normal service as quickly as possible, while minimizing impacts to operations. As an example, consider an engineering department seamlessly switching to battery backup power without impacting the user during a power spike.

Request Fulfillment and Access Management. Service requests are requests from users for information or advice. Based upon roles or positions within an organization, access is granted to appropriate services and resources. The network architecture and permissions should be structured accordingly to accommodate an organization's unique needs. Security principles such as least privilege help with this process to manage confidentiality, integrity and availability of IT resources.

Problem Management. Alison Cartlidge further states that "a problem is a cause of one or more incidents. The cause is not usually known at the time a problem record is created, and the problem management process is responsible for further investigation" [12]. The problem management process attempts to identify and resolve the source of a problem. A primary goal of this process is to reduce the number, severity and duration of incidents. An efficient problem management process identifies and prevents incidents prior to them occurring.

2.5 Continual Service Improvement

Continual service improvement is a process that focuses on maintaining optimal customer service through constant improvement. Evaluation of current processes and determining better methods for performing tasks is the value added component to this process. Continual service improvement combines several functional areas for improving the overall IT management process (see Figure 4). Accordingly, the primary processes are partitioned into service measurement and reporting, a seven step continual improvement process, and service level management.

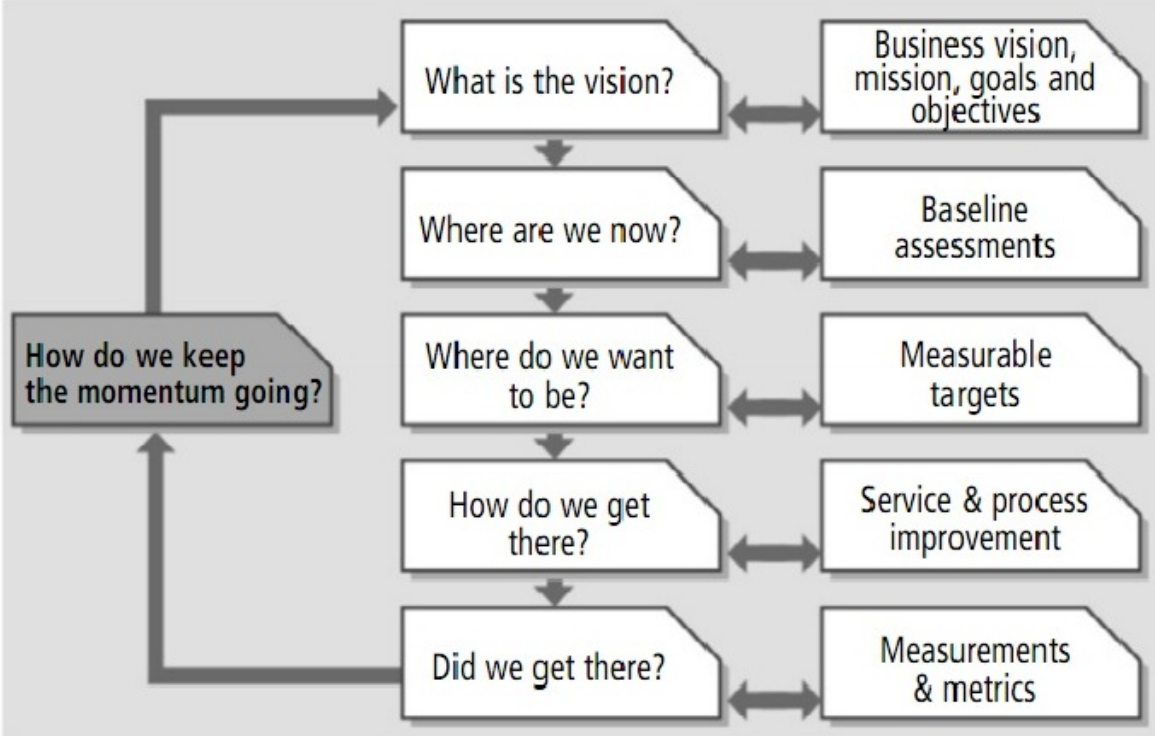

Figure 4: Continual Service Improvement Process

Service Measurement and Reporting. Over the course of a business day, a large quantity of information is collected and stored in archival logs. Performing trend analysis on that data is a valuable component to leadership making informed decisions. Quarterly metrics on efficiency of operations and identification of repeat issues are critical. Overall, service reporting examines *who, what, when, where, how* and *why* based on historical trends. The analysis helps identify the necessary steps to mitigate any reoccurring problems. An indicator that an organization is failing to learn lessons from historical trend data becomes apparent if the process demonstrates continual issues.

Seven Step Continual Improvement Process. There are seven steps associated with collecting tangible data to implement improvement. Figure 5 demonstrates the process and identifies the attributes of each specific step. Note that defined and measurable goals from leadership are a critical aspect of this process.

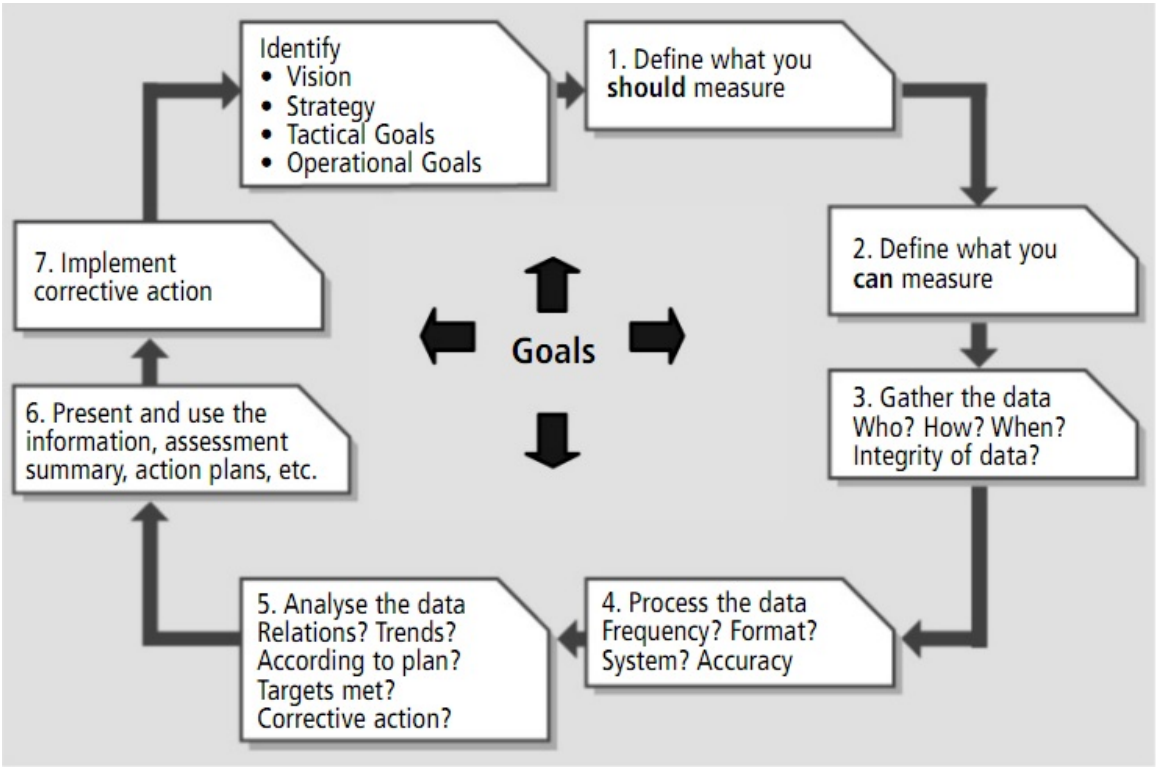

Figure 5: 7 Step Process Improvement Process

Service Level Management. Service level management is the process of continuously examining IT services. This overarching process examines the established IT structure and monitors performance and adequacy of IT services. If necessary, the expansion or reduction of capabilities may need to occur to align with an organization's current operations and long-term goals.

2.6 Conclusion

This chapter examined the ITIL process and described attributes for three of the core publications. These attributes form the basis of analysis for identifying shortfalls and recommendations with respect to current Air Force network operations.

III. Air Force Network Operations Center (AFNOC)

This chapter examines the current construct of IT service management for Air Force Network Operations (AFNetOps).

3.1 Transition

Prior to the AFNOC becoming operational, bases operated independently and reported directly to the MAJCOM/A6 for network decisions. There was no true standardization between the MAJCOMs and operations were implemented in a centralized control, decentralized execution construct. Upon receiving the execute order, the Air Force stood up the Air Force network operations security center (AFNOSC), later renamed the AFNOC. The AFNOC worked directly for the AFNetOps commander and ensured the networks were capable of conducting, supporting and advancing coalition, joint, Air Force and inter-agency operations. Additionally, the customer was provided situational awareness, command and control as well as vulnerability, patch and virus management. The AFNOC also released time compliance network orders (TCNO), network tasking orders (NTO) as well as mission tasking orders (MTO) (see Figure 6).

Today, the AFNOC has dissolved; however, the functions have been migrated into areas within the 624th OC (See Figure 7). Administrative control (ADCON) responsibility is directed from AFSPC, 24th AF, 67 NWW, 690 NSG to the NOS, respectively. For operational control (OPCON), the authority is similar with the exception that the 561st NOS, 83rd NOS, 299th NOSC and AFCENT NOSC report directly to the 624th OC, 24th AF, US Cyber Comm, and then USSTRATCOM. The combat plans, operations, intelligence, surveillance and reconnaissance divisions within the 624th OC receive strategic guidance for all tasking orders and FRAGOs, then delegates them to the I-NOSCs. Note, a FRAGO is an operational surge in capability that directs the military sources to fill a capability gap.

The I-NOSCs comprise the two regional NOSCs, with detachments that were the former MAJCOM NOSCs (see Figure 8. This organization stemmed from the

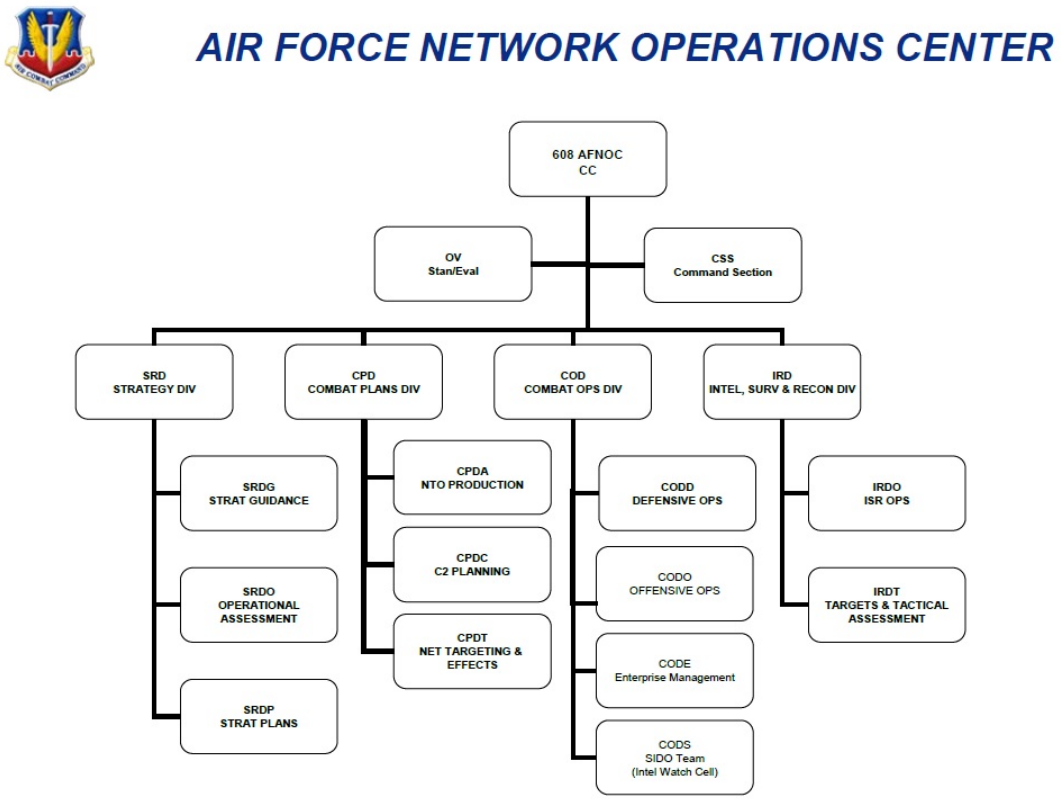

Figure 6: AFNOC Org Chart

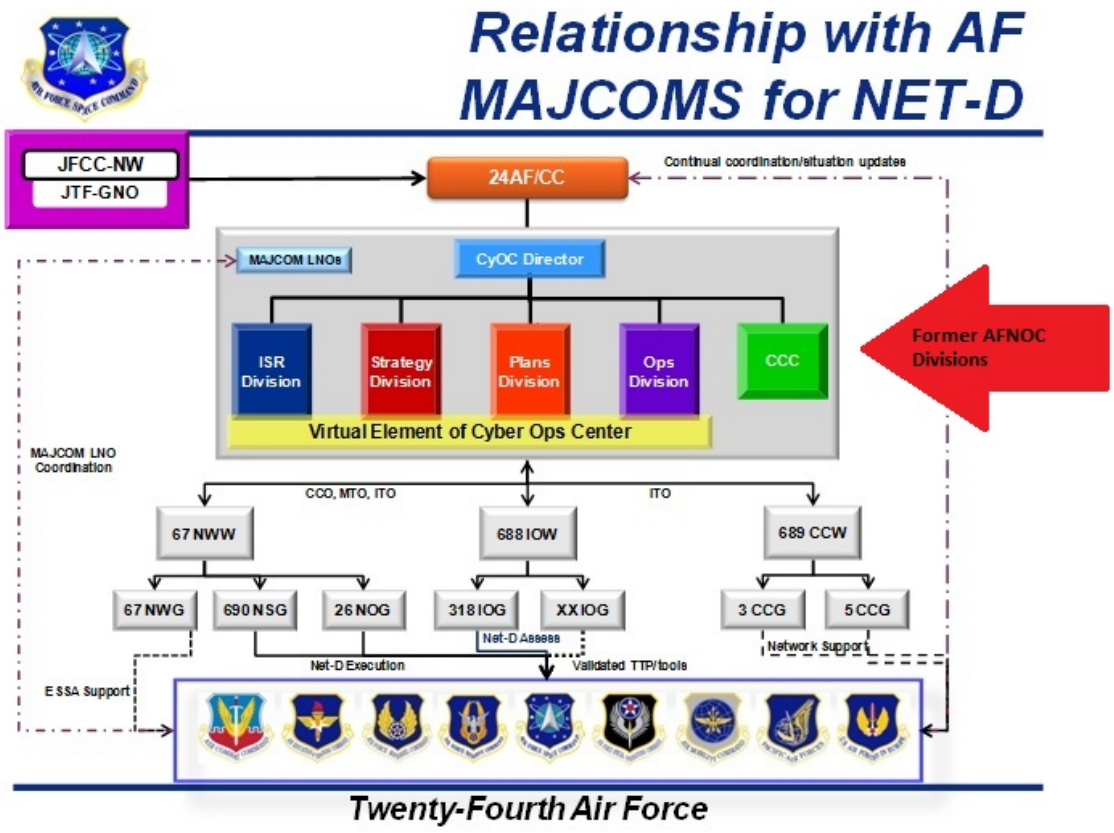

Figure 7: 24th AF Structure Current as of 16 May 2011

MAJCOM NOSCs lacking unity of command, no unity of effort and a lack of standardization at the base level. Detachments are considered to be an enterprise service unit (ESU) and provide the following: directory and authentication Services (Active Directory, PKI, etc.); email management, mobile services (e.g., BlackBerry, WinMobile); web services hosting web applications; organizational messaging (e.g., AMHS); collaboration services (e.g., SharePoint, OCS); network management and monitoring tools;storage area networks; and virtualization. The detachments are located at Hickam AFB, Peterson AFB, Langley AFB, Ramstein AFB and the ANG NOSS [13]. Prior to realigning under the 24th AF, their focus included the following: AFNetOps command authority to secure and operate the AF-GIG; conduct network monitoring and control via 24x7 operations; deliver situational awareness to the AFNOC via network monitoring; reporting, escalation and notification; remote administrative net infrastructure; provide monthly vulnerability scans; perform directed scheduled maintenance; and execute NTOs/MTOs, TCNOs and Fragmentary Orders (FRAGO). Indeed, the central role of the I-NOSCs is summarized as captured by the 2006 I-NOSC Tiger Team:

> "Vision: Act as a key node in an AF network control system through real-time and effective Command and Control (C2) over the AF provisioned portion of the GIG.
>
> Mission: The execution arm of the AFNOSC performing C2 and supporting shared situational awareness to accomplish enterprise management, network defense, and content staging for the AF provisioned portion of the GIG, ensuring AF networks are capable of conducting, supporting and advancing coalition, joint, AF and inter-agency operations" [14].

The other network operations unit examined in this research is the 299th NOSS and they are members of the Kansas Air National Guard. The 299th NOSS is located at McConnell AFB and is the I-NOSC equivalent for the Air National Guard (ANG). The 299th NOSS provides the same services and reporting as the two primary I-NOSCs. However, the chain of command follows two distinct paths. A portion responds on orders levied by USCYBERCOM by way of the 624th OC and the 24th AF. The other portion follows a traditional path of direction and reports to the

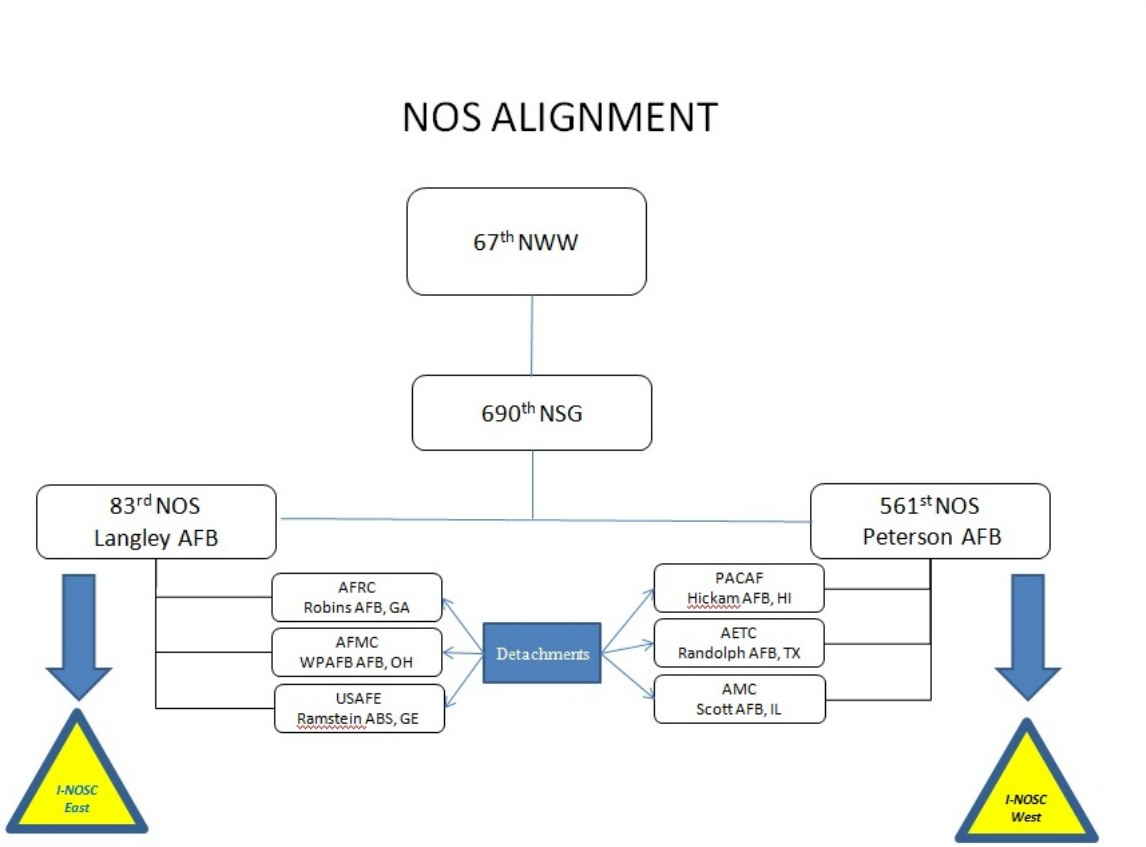

Figure 8: Current NOS Alignment

Regional Support Group of the 184th Intelligence Wing who works for the Adjutant General (TAG) of Kansas. They manage network defense; generates an enterprise situational awareness picture; manages network configuration; provides information assurance for all ANG networks. [15] They also serve as the network help desk for application and system issues throughout the entire ANG enterprise (See Figure 9).

3.2 Diversity

There is an inherent lack of standardization across the AFNetOps enterprise for managing network operations. For example a disaster recovery plan (DRP) is essential to ensure continuity of operations for any organization. The DRP typically outlines a return-to-operations strategy, including the detailed steps. The DRP should be exercised and tested to ensure the organization is ready to execute the fail-over plan in the event of a disaster. Other than slight differences due to geography, basic service should still be available regardless of where the company is located. With respect to the I-NOSCs, there is no readily defined DRP for failover in the event of a major crisis. To date, only the phones have been successfully failed over.

Upon completion of the AFNet migration, this issue, however, should be resolved. Once the AFNet and active directory exchange (ADX) is implemented, the Air Force will experience a transformation of cyber operations resulting in the following: reduced operating and maintenance costs; greater collaboration capabilities; and enterprise-wide standardization. The most notable benefit will be the ADX initiative, which enhances network and remote email access and improved management for the global access list (GAL) [16]. Additionally, the single sign-on capability for all bases will enhance exchange posture and support standardization across the GIG. This initiative stands to improve AFNetOps and further validates the movement towards full COOP capability. To date, the Air Force has completed AFNet Increment 1, which assisted combat information transport system (CITS) Block 30 for Air Force gateway consolidation. This initiative reduced the 104+ bases with standalone gateway connections (i.e., points of presence) down to 16 gateways.

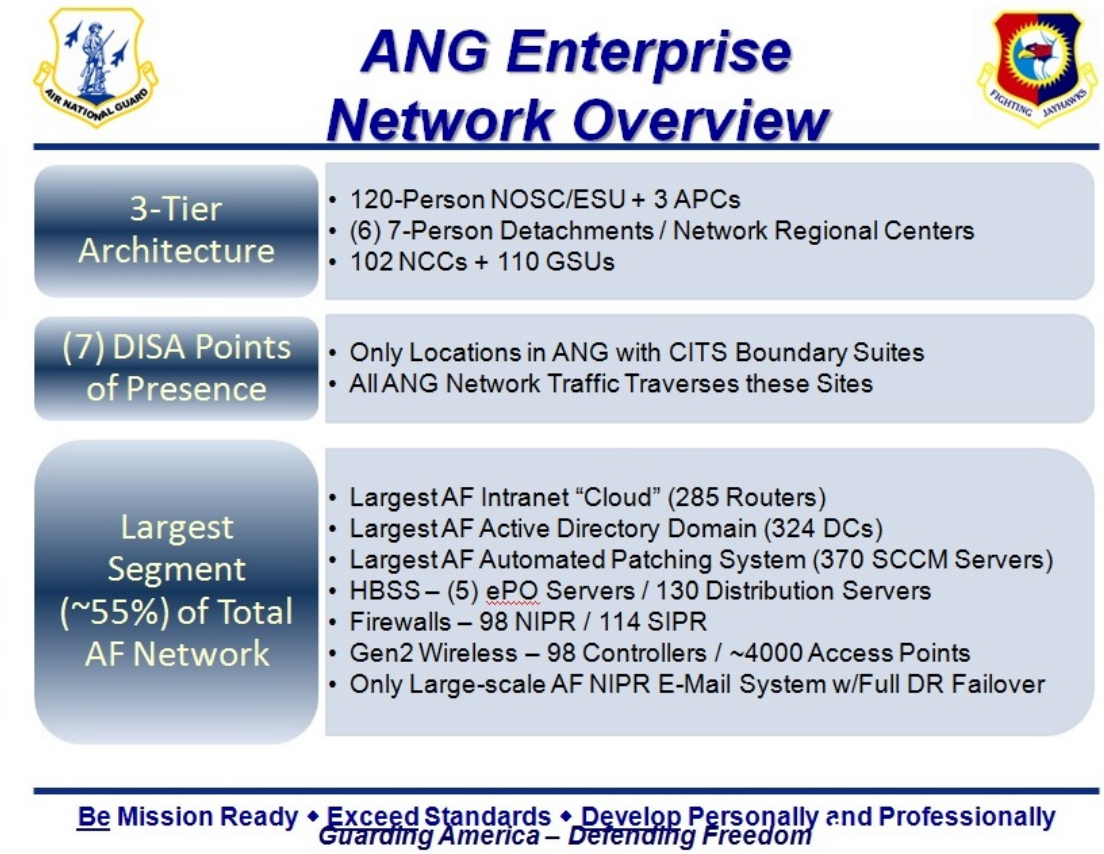

Figure 9: ANG Enterprise Network Overview

> "The AFNet being built today will consolidate network application and help desk services that are operating independently today! By consolidating these networks and centralizing services, we can reduce our manpower and equipment footprint and still deliver the mission support our customers need." - Col Donald Locke, Commander, 690th Network Support Group

3.3 Centralized Control, Centralized Execution

The AF has experienced success with centralized control, decentralized execution through other domains. Joint Pub1-02 (JP1-02) defines centralized control as "Placing within one commander the responsibility and authority for planning, directing, and coordinating a military operation or group/category of operations" [17]. Air Force doctrine clarifies JP1-02 with the additional verbiage, "The planning, directing, prioritization, allocation, synchronization, integration and de-confliction of air and space capabilities to achieve the objectives of the joint force commander" [18]. Decentralized execution is defined jointly as, "Delegation of execution authority to subordinate commanders" [17]. The AF injects additional verbiage to include, "Decentralized execution of air and space power is the delegation of execution authority to responsible and capable lower level commanders to achieve effective span of control and to foster disciplined initiative, situational responsiveness, and tactical flexibility" [18]. If you look back about ten years, the Air Force used decentralized execution for network operations; however, the responsibility involved decentralized control as MAJCOMs had their own director of communications.

The advent of the AFNetOps has provided a road map for a way ahead. Over time, operations have shifted in the direction of centralized control, centralized execution. Indeed, US Cyber Command has been designated the lead agency for all things Cyber [19]. The command structure issues taskings that flow to the I-NOSCs through the 24 AF and 624 OC for execution. However, execution has been assigned to I-NOSCs rather than base-level squadrons.

3.4 Complex System

Traditional network control centers of communication squadrons had difficulty managing systems on their respective bases. This problem was exacerbated by the roll up to their MAJCOMS and ultimately to their respective I-NOSC. Indeed, span of control increased complexity by the number of MAJCOM bases under each I-NOSC umbrella. New systems had to be purchased to manage the complexity, each warranting subject matter expert to operate them. Due to their complexity, permanent change of station movements, and deployments, the overall effectiveness was severely degraded. Constant changing tactics, evolving system structure and network probing/attacks from every angle warrants up-to-date patching, monitoring and change management reviews. With the speed that technology is evolving and new systems brought online, it can be assured that someone is already trying to circumvent defenses for malicious actions. Time is not a luxury. However, the I-NOSCs have to wait for certification and accreditation process to validate any new security systems. How do these various issues effect the overall mission set of the Air Force? Fortunately, analysis of how IT management aligns with organizational goals can limit the impact to these challenges.

3.5 Conclusions

This chapter explained milestones that led to the creation of the AFNOC, its assimilation into the 24th AF and the gun camera view of the relationships amongst the NetOps execution units. It also explained some of the organizational structure of the NetOps squadrons as well as some of the challenges they face. These organizations comprise a significant line of defense of our posture in maintaining C2 and defending our networks.

IV. Merging ITIL into I-NOSC Operations

Since the inception in the 1980's, companies have adopted the ITIL framework of best practices for delivering IT services and joined the myriad success stories. The United States Air Force recognized these successes and began incorporating ITIL processes in 2004 [20]. Indeed, Air Force Instruction 33-115 Volume 1 identified the incorporation of ITIL into network operations as it provides "overarching policy, direction, and structure for the Air Force Global Information Grid (AF-GIG) and procedures necessary to manage the increasingly complex network environment" [21].

This chapter examines Air Force network operations (AFNetOps) with respect to the ITIL process. The analysis focuses on the two I-NOSC squadrons. Additionally, discussion of the Air National Guard NOSS (I-NOSC G) is provided.

4.1 The Air Force I-NOSCs

The 83rd NOS and 561st NOS run the I-NOSCs and are the primary Air Force squadrons tasked with daily execution of defensive network operations. Each squadron is comprised of active duty, civil service and contractor personnel. This section examines the two squadrons according to the following ITIL principles: service transition, service operation and continual service improvement. I-NOSC teams have been working for over a year to incorporate the five ITIL volumes into the IT management lifecycle for the Air Force (see Figure 10).

4.1.1 Service Operation. Service Operation is charged with delivering the agreed upon levels of services to users and customers as specified in the I-NOSC and AFNetOps implementation plans. The primary goals are stability of the enterprise, quality of service to users, and internal view. This is the core of all I-NOSC functions. Not surprisingly, tasks associated with service operation can be difficult and overwhelming.

Event Management: The ability to find root causes of an issue and develop a database for historical analysis is currently lacking. The ITIL SME indicated that

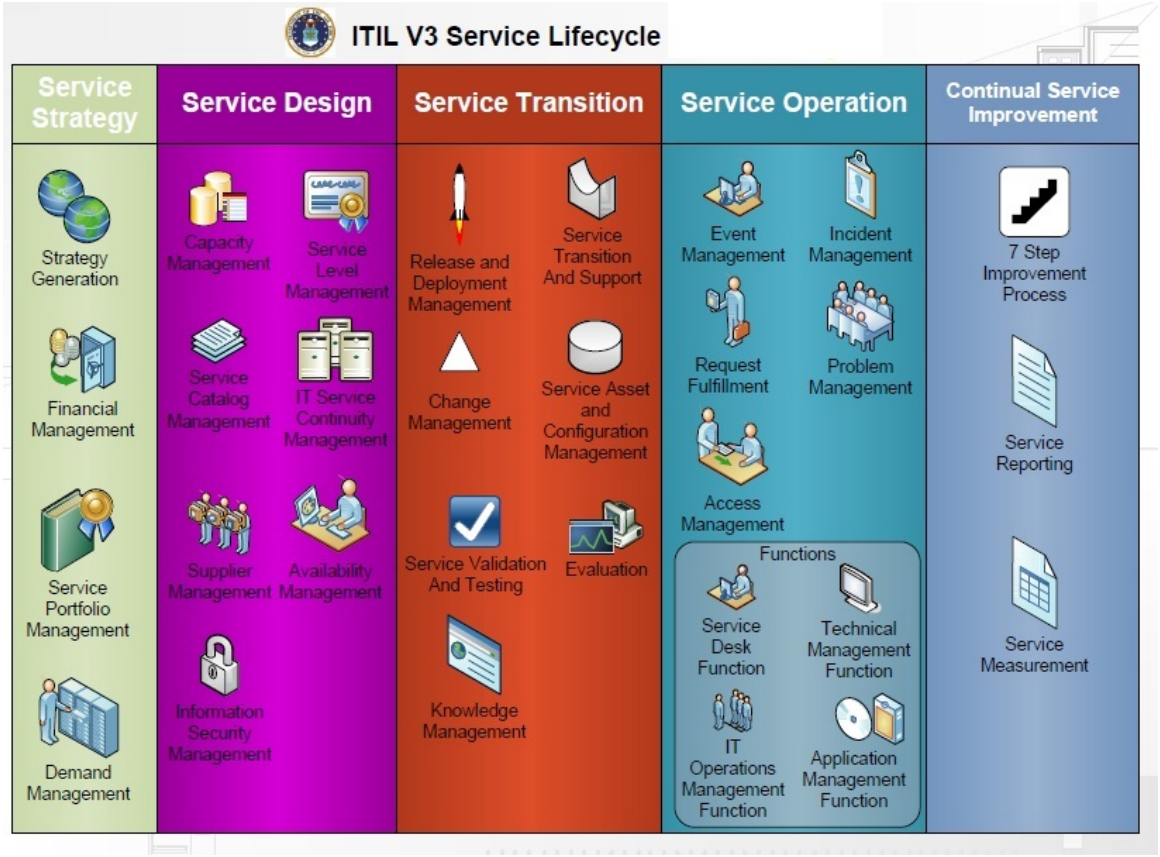

Figure 10: ITIL Service Lifecycle [1]

there is a large amount of information captured daily within log files at the 561st and 83rd NOS, it was indicated that because of daily taskings and operations work flow that manning is not sufficient to provide the service necessary for forensic analysis of that data. Additionally, the DOV an/or Stan Eval sections are performing correlation for critical problems as well as accomplishing after action reports. Although each of these units are working to improve their commitment, however, they are not devoting adequate emphasis to this area. As a result trend data is not appropriately analyzed.

Incident Management: Incident management requires a day-to-day approach. The crew commanders are responsible for prioritization and performing incident management to restore services as necessary. For determining authorized service interruption, decisions are made based on service availability, as opposed to priority of mission impact. Additionally, CTO's are not prioritized due to potential impact, with the exception being the most critical circumstances.

All MTO's that are processed originate as cyber control orders, unless immediate situations dictate otherwise. Impacts to potential mission sets are coordinated and controlled by crew commanders who have the authority to cancel anything that may be detrimental based on operations. After discussing this area in depth with the director of operations, crew commanders and operations controllers at both units, the I-NOSCs are performing this task admirably. They realize the importance of this task and have an aggressive approach for accomplishing this area. Additionally, the professionals this research received inputs from stated that this is by far the most mature area within all of the units.

Request Fulfillment: All functional areas within the I-NOSCs contribute to request fulfillment. If there is a change submitted, they ensure follow-up actions are taken. Additionally, a large portion of personnel during the site visits were observed performing this task throughout the day. Rules and permissions are identified and adequate access is assigned accordingly. The concept of least privilege and need to know are fairly substantiated throughout the IT service management process. How-

ever, it should be noted that 83rd NOS appeared more aggressive than the 561st NOS for executing this task.

Problem Management: The Stan Eval section performs the majority of problem management for the I-NOSCs. The small section is responsible for determine the root cause of an incident and identifying and systemic issues. For example, within Remedy 7.1 (process for tracking trouble tickets), there is a component that can be leveraged to correlate reoccurring issues. However, per the 561 NOS ITIL SME, the data is only sufficient if adequate information is entered, which is the primary shortfall identified for problem management. The 561st NOS is not as mature in this area as the 83rd NOS but are working towards improving their posture.

4.1.2 Service Transition. Each service transition functionality of the I-NOSCs utilize the Plans and Programs section for this area. They coordinate closely with service design across the life-cycle area of IT management. Organizationally, the CITS office is in charge of bringing the systems into the organization. This area works with the Systems Telecommunications Engineering Manager Command Lead (STEM-C) who provides technical assistance to the MAJCOM and coordinates with STEM-Bs (base-level) on future MAJCOM mission changes, programs and efforts. A close relationship between these agencies is crucial to long term planning. As an example, the 561st NOS is currently working on fully integrating all of their Service Transition and Operations into the ITIL v3 Process Flow see Figure 11. If this process is closely followed, achieving optimal service is well within each of the squadrons' grasp.

Transition Planning and Support: Transition planning and support is a maturing capability for the I-NOSCs. As an example, the 561st NOS is directing a large portion of this effort into responsibility definition and creating process documents for task execution. TO 00-33A-1100 is in draft but it addresses network dependency diagrams and defines tactics, techniques, and procedures as they apply

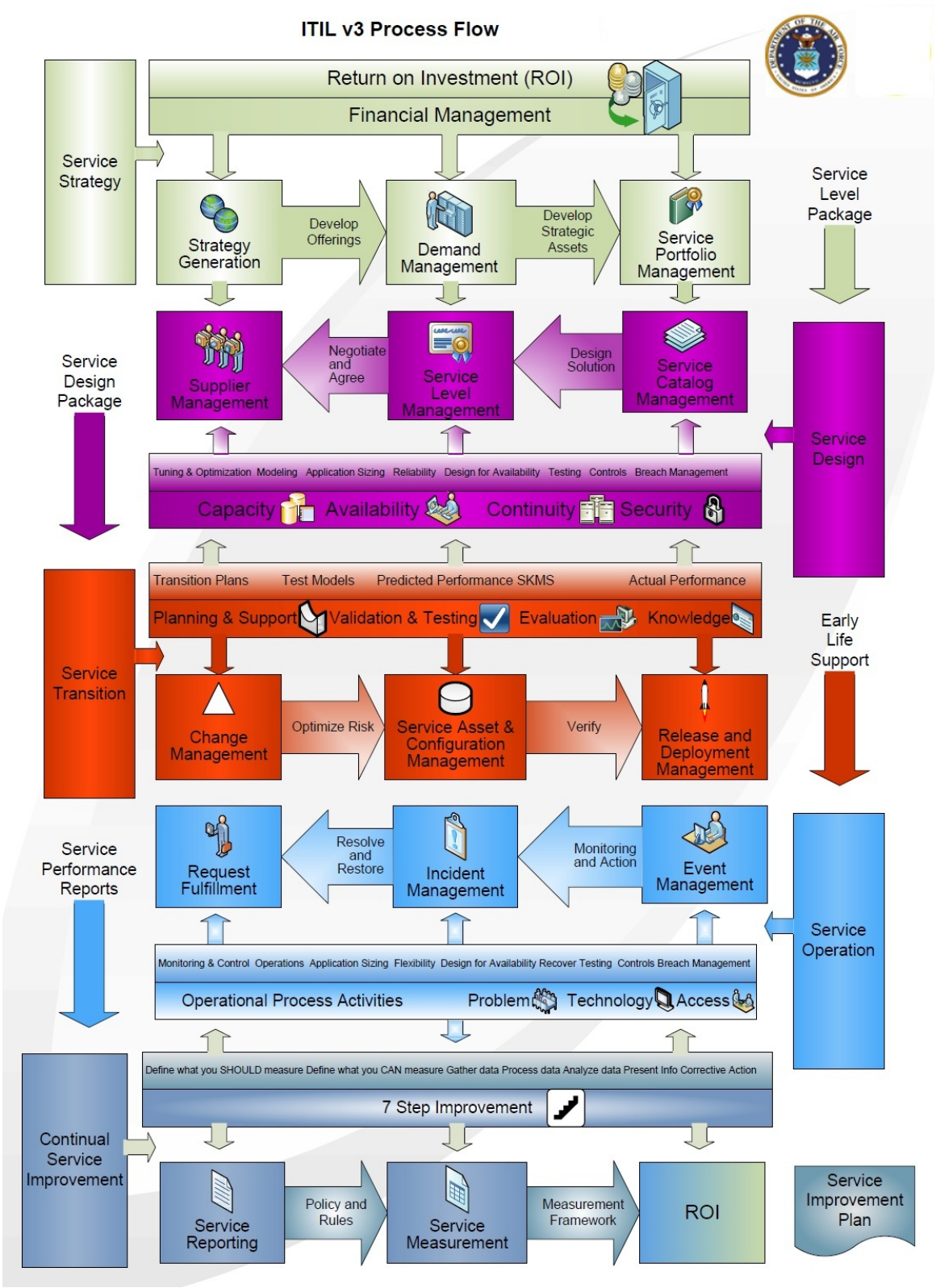

Figure 11: 561st NOS ITIL Process Flow [2]

to a change. Detailed processes were also created and used as checklists for performing change management and for processing a change request.

Change Management (CM): This is the focal point for the Plans and Resources section within the I-NOSCs. The standard change plan according to TO 00-33A-1100 (see Figure 12) and the minor/significant/major change process flow (See Figure 13) are outlined according to set criteria. Mission requirements are the driving factor for determining the appropriate guidance that should be followed. For the 83rd NOS, there appears to be minimal push-back from units when necessary changes must be implemented. As a side note, the 624th is identified as having a change advisory board, however, the function was not implemented during the time of the site visit. The 24th AF does have a change management board in place, but full awareness of the impacts to units is difficult to ascertain at such a high level. In short, impacts of second and third order effects are not fully researched down to the appropriate level.

During the draft conference for TO 00-33A-1000, attendees were asked if there were any requests. Members from both I-NOSCs responded that understanding the change management process was critical. Awareness of implications for forced changes was necessary for ensuring sustained and adequate network operations.

Service Asset and Configuration Management: Service asset and configuration management is a focus area for the I-NOSCs. Currently there is movement to fully incorporate automated tools to aid in asset management. The full release of Remedy 7.1 contains an array of automated toolsets that greatly improve this area. The discussions with the ITIL SME's from the 561st NOS indicated that this process is currently at 50 percent maturity.

As an example of change management, consider an MTO that is issued to update the latest version of a software package. A change request process must be accomplished before a technician is allowed to execute it. Additionally, patches are the most common aspect that requires a change request. However, FRAGO's typi-

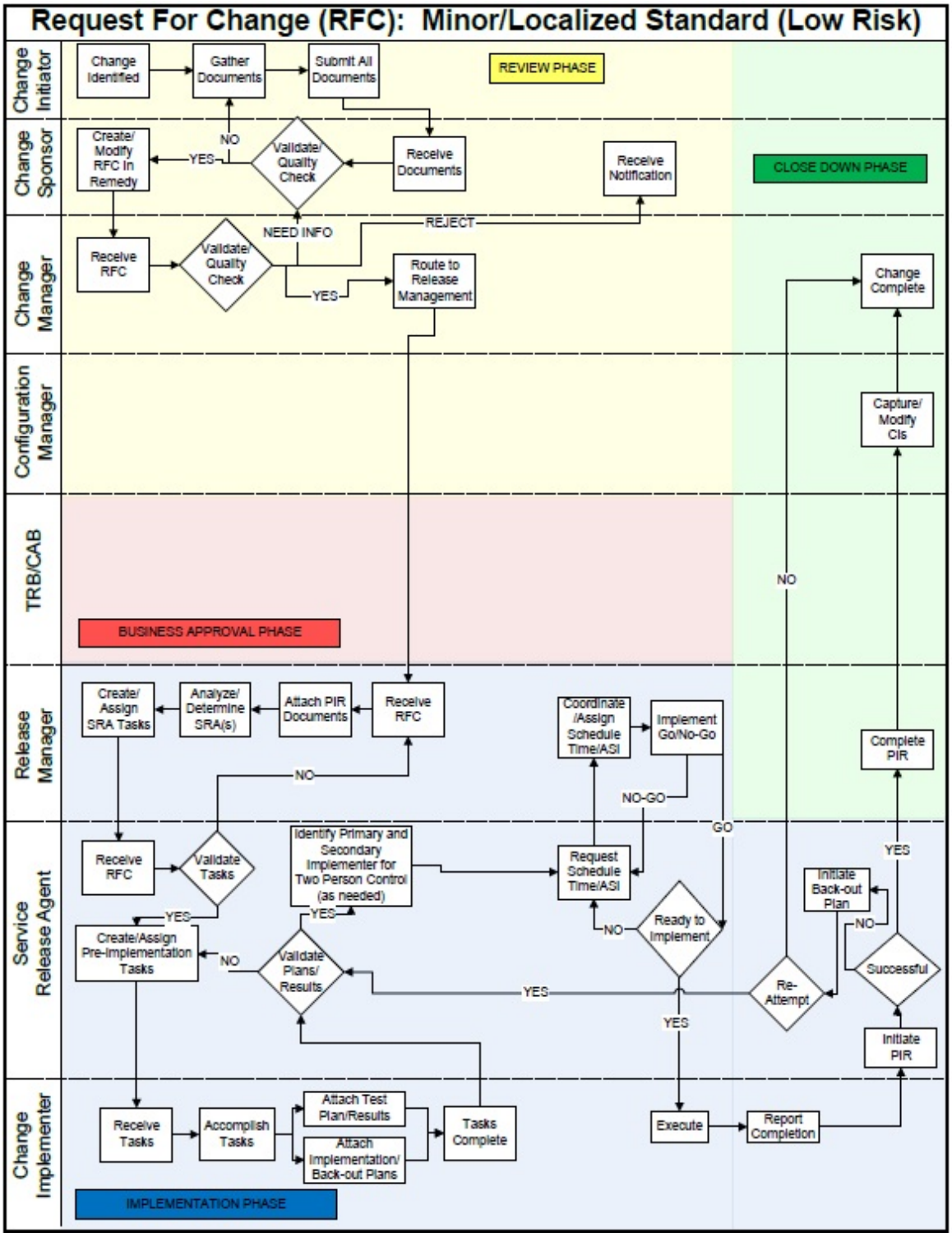

Figure 12: Request for Change Low Risk [3]

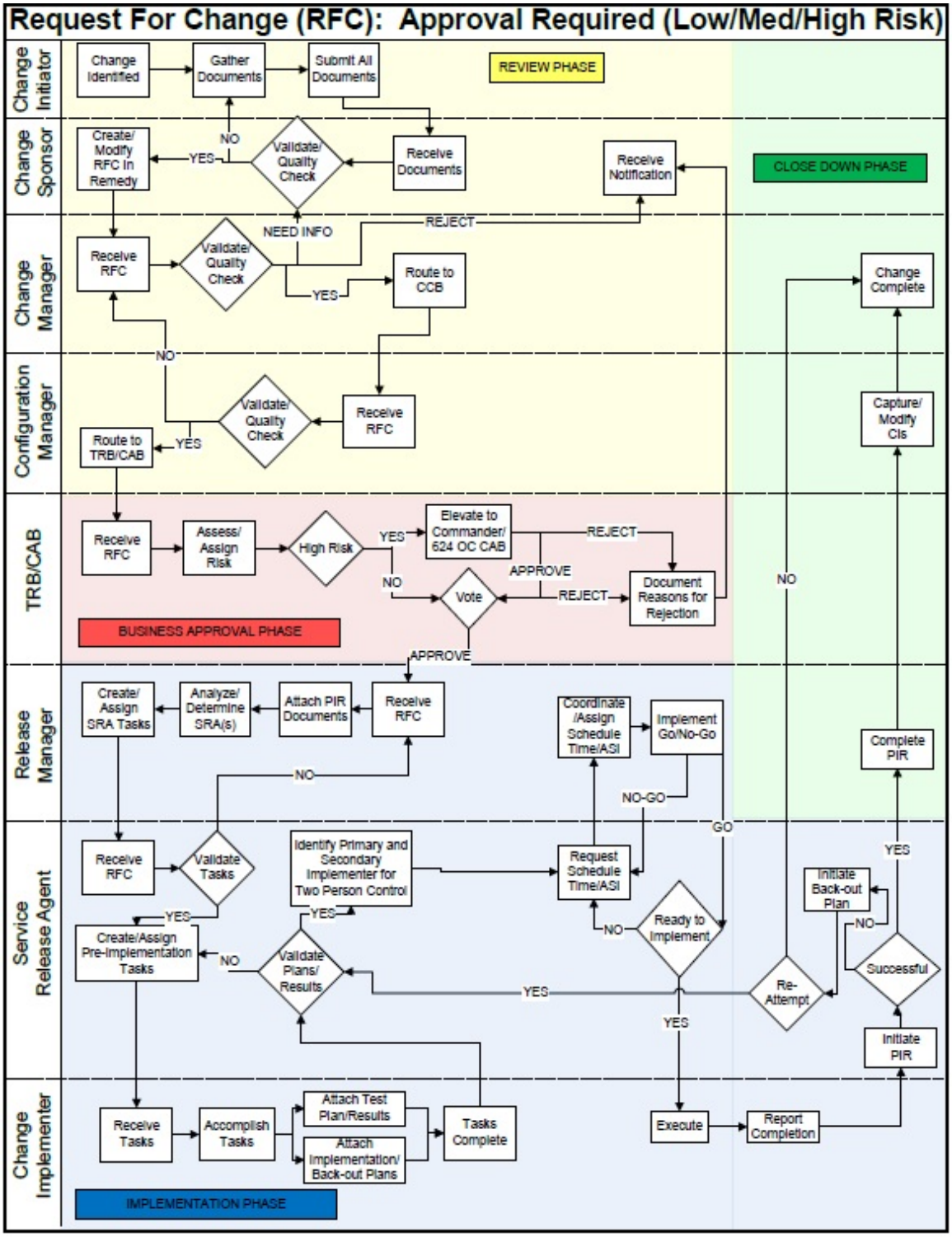

Figure 13: Request for Change, Approval Required

cally address a critical vulnerability and are issued via a Cyberspace Control Order (CCO) which dictates immediate implementation. Once the change is implemented, the technician documents the change.

Release Management: This section focuses on de-conflicting the schedules for releasing changes to network resources. The INOSCs have invested heavily in this functional area. Customers submit a request for service support at a specific time based on mission requirements. Release management processes ensure the patch mission is not dependent on a network segment or resources that are blocked or currently unavailable.

For planned maintenance and downtime, users expect services returned and completely operational at a specified time. If the process can not be accomplished within the specified time-frame, maintenance is expected to roll back the change and schedule for another time. Obviously, critical actions are an exception. Additionally, lack of standardization across the network has negatively effected release management. For example, a task may mandate that every system must use the latest version of a software application; however, over 5,000 different configurations or versions exist and the impacts are not well known for each implementation.

Service Validation and Testing: Before CTO's and MTO's are tasked to the I-NOSCs for implementation, they should be tested and validated. However, this formal process is quite limited. For example, the 83rd NOS has a section that must build, test and deploy every tasking order. AFNIC stated they have a testing lab and have been invited by the I-NOSCs to become a part of the coordination piece. In this case, 24 AF will deliver the tasking order to AFNIC which will test and validate via their lab before pushing to the I-NOSCs for implementation.

Evaluation: Upon execution of the tasking order, the I-NOSC must evaluate the effectiveness. Both I-NOSCs currently lack a formalized documented method. Currently, the organizations rely on user feedback to determine if the tasking order breaks something. It should be noted that this issue was a priority for both I-NOSCs.

Knowledge Management: Knowledge management ensures that the right person has the right knowledge at the right time to deliver support and services required by the organization. This goes hand-in-hand with the recommendation for all Air Force cyber professionals receiving ITIL foundation training at the earliest part of their career and refresher training every other year. As previously mentioned, technology changes rapidly and cyber professionals must understand that the initial training they receive is only the beginning of their education and training.

4.2 Analysis of the I-NOSCs

The site visits allowed insight into the overall perspective of the individuals responsible for managing the Air Force's IT processes. Overall, the 83rd NOS feel that they were doing a good job, but understand there is room for improvement. Since 2004, the improvements in change management allowed the 83rd NOS to reduce major network incidents by 47 percent while coordinating more than 1,100 successful network changes [20].

Years ago, the 561st NOS realized that they needed help within their organization for change, release and configuration management in relation to how the 83rd NOS was postured. The 561st NOS only had four personnel compared to fifteen at the 83rd NOS. At that time, the ITIL subject matter expert submitted an unfunded request for $1.5M per year to plus-up the staff so they could be equivalent with the 83rd team. Twelve personnel were hired, with one person as the ITIL expert. Currently, they have three ITIL experts to continue the initiative.

Both I-NOSCs are taking steps to assist other network operation squadrons with their ITIL posture. For example, they are assisting change management personnel at Detachment 2 (Hickam AFB) get trained and certified. Additionally, extensive documentation has helped in standardization across AFNetOps.

4.3 The 299th NOSS

The 299th NOSS is located at McConnell AFB and is the home to the Air National Guard NOSC. Their ITIL process is somewhat more mature than the two I-NOSCs, primarily due to the fact that they have been practicing their methodology since 2004 and have minimal personnel turnover rates. This section briefly discusses a subset of the ITIL process areas for the 299th NOSS. The goal is to highlight the differences in the the ITIL processes.

The 299th NOSS has fully integrated incident management into operations. They do not have one incident manager or one service desk for this aspect, rather each section coordinates for their respective area. Once an incident occurs and is resolved, the solution is shared across the community via a common reporting mechanism. For request fulfillment, the 299th NOSS utilizes standard processes and metrics to provide leadership information on service levels. The 299th NOSS is unique in that they track both events for incident management and service requests independently.

The I-NOSCs use federal funding under Title10 authorities for service transition and acquisition. The 299th NOSS, however, receives state funding through Title 32 authorities. Because funding lines are different, the possibility exists for non-standard equipment/resources across the Air Force as a whole. To help mitigate this potential problem, the 299th NOSS incorporates AFNIC on acquisition processes to ensure a comprehensive certification and accreditation is accomplished prior to implementation. Additionally, the 299th NOSS uses the technology and integration section as the primary liaison to the National Guard Bureau (NGB). Coupled with support through AFNIC, they help coordinate efforts with the NGB so that there is an awareness of how new equipment resources is going to effect the end-state and who is primarily responsible for supporting it. The technology and integration sections also act as liaisons to the I-NOSCs and other primary network operations units to help oversee and integrate any initiatives.

The 299th NOSS leverages a replica network for validation and testing of new services, updates and equipment. The environment enables testing and validation of directed changes prior to implementation on the operational network. A lab manager oversees the environment and can produce metrics upon request. Less than a year ago, a quality assurance section was implemented and tightly coupled to the Stan Eval section. The integration enables hardware and personnel evaluations for any new system that is scheduled for employment on the network. This process helps identify shortfalls in both capabilities and personnel training.

Finally, the 299th NOSS leverages an application for knowledge management that allows any IT person to create an article and share it across the enterprise. For example, If an individual identifies a resolution to a Windows Vista problem, they can create a knowledge article and share it with the rest of the enterprise through a common platform. This notion builds a significant body of lessons learned and is a vital resource for researching problems. The process works by an individual creating a knowledge article and submitting it through the system. A subject matter expert in the knowledge management section is designated to review the submission. Once reviewed for technical validity and formatting, the article is published to the community. After a one year time frame elapses, the author and knowledge management section are notified to see if it is still valid, needs to be updated, or needs to be retired.

The ITIL program at the 299th NOSS is fairly well established. The lessons learned and implementation are a resource for the I-NOSCs to leverage. Indeed, the processes that the 299th NOSS have in place demonstrates their commitment to providing excellent customer service and support to reporting units. Each section that was interviewed showed pride and dedication in their functional areas. Throughout the site visit, there were multiple calls from field units regarding issues, outages and a host of other situations that were handled professionally and in accordance with established ITIL processes. The 299th NOSS appeared to be a cohesive unit and the value of ITIL can be seen in how the members perform their daily operations. Most

importantly, it was evident that there is managerial buy-in to the ITIL process which is crucial for success.

4.4 Conclusions

This chapter examined functional areas within Service Operation (SO) and Service Transition (ST). The components examined were pieces of the set of 5 ITIL Service Lifecycle stages that operates where the user interfaces directly with the service provider. The three NetOps units have adopted the ITIL framework into their organizations but are at different levels of final operating capability. The SME's on staff realize that in the aforementioned areas of SO and ST, ITILv3 Process Flow is the place where you can make or break the squadron. Collaboration amongst the squadrons have occurred as evident in the collective draft TO 00-33A-1100 AFNetOps Operational Change Management Process. Within this chapter, components of this TO is being exercised while area teams within each squadron work to improve the process.

V. Recommendations

The chapter provides recommendations based on shortfalls identified in the ITIL process and various insights gained from discussions during the site visits. The goal is to provide leadership with suggestions for improving the overall AFNetOps IT management posture.

5.1 Restructure 67th Network Warfare Wing

The 67th NWW is charged with the mission to execute AF Network Operations (AFNetOps) defense, attack and exploitation to create integrated cyberspace effects for the AFNetOps commander and combatant commands [4]. Their current structure consists of the 26th Network Operations Group (26th NOG), 67th Network Warfare Group (67th NWG) and the 690th Network Support Group (690th NSG). The groups are a composed of network warfare, network operations, network support and operations support squadrons. The current 67th NWW structure has the 26th NOS under the 26th NOG while the 561st NOS and 83rd NOS are aligned under the 690th NSG; however, they perform the same functions. Unfortunately, this type of hybrid organization is detrimental to IT management processes. As a recommendation to support ITIL processes, a reorganization similar to the structure identified in Figure 14 is recommended. The proposed structure identifies the similarities amongst the squadrons and aligns them for maximum efficiency.

The 26th NOG "Operates the Network" by ensuring C2 functions are not interrupted and the networks are capable of conducting, supporting, and advancing coalition, joint, AF, and inter-agency operations [22]. Those functions are currently carried out by the 26th NOS, 561st NOS and the 83rd NOS. The 315th NWS and the 91st NWS perform network attack functions while the 33rd NWS, 68th NWS and 352nd NWS perform traditional network defense functions and will "Fight on the Network" within the 67th NWG. Maintenance functions are carried out by the 690th NSG and consist of enterprise service units from Hickam AFB, Ramstein AB, Langley AFB, Peterson AFB and the 67th Network Support Squadron and they will

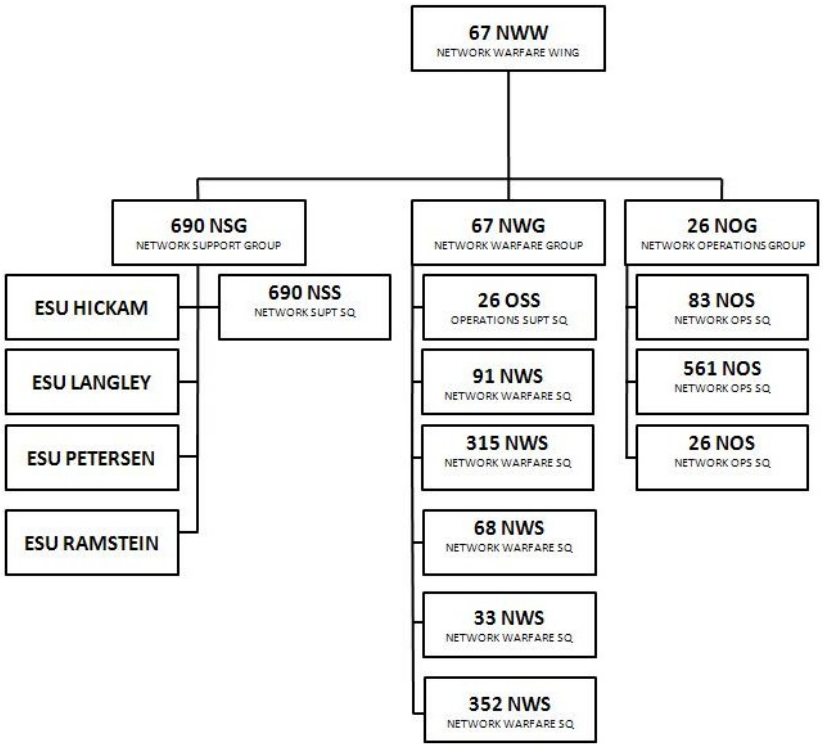

Figure 14: Recommended 67th NWW Structure

perform "Maintenance on the Network." (Col Kevin B. Wooton, Commander 67th NWW) Enterprise service units migrate responsibility of network core services from the inconsistent standards to a consolidated facility responsible for monitoring and management 24 hours a day, 7 days a week, 365 days a year [4]. The 690th Network Support Squadron is the enterprise service desk (ESD) and the AF-level, first-response service desk management for all core services [23]. The ESD is responsible for:

1. Maintaining incident control managing the life cycle of all service requests routed through the ESDs
2. Upon request, update customer and advise on approved work arounds
3. Troubleshooting and attempting incident resolution for incidents affecting base users that cannot be resolved by CSA/CSTs, FSAs, and/or CFP personnel
4. Interface with appropriate Tier 2 entities for incident resolution
5. Maintaining situational awareness of the AF-GIG to help determine trends and begin assessing problem/incident management
6. Making final contact with end user to confirm adequate resolution for closure of service requests
7. Monitoring the NOS Dashboard for higher level outages and service request updates
8. Administering AD objects as authorized and provide remote desktop administration/assistance

5.2 Education and Leadership

Air Force IT managers must be educated on the benefits of ITIL at the earliest point in their careers. Disney took this approach in the early 2000s and trained 250 of their personnel. Of the 250 trained personnel, 50 percent elected to take the official ITIL certification test, with a 100 percent pass rate [6]. Although the same scale may

not be necessary for the Air Force, formal training and ITIL certifications mandated for network operation squadrons would vastly improve Air Force IT management.

Additionally, Air Force leadership should advocate for ITIL practices incorporated throughout IT management lifecycle. This notion ensures organizational commitment and buy-in. For example, the Internal Revenue Service (IRS) committed to the ITIL process and implemented a five-year strategic plan from 2009 - 2013 [24]. The IRS recognized that in order to succeed in meeting their goals, they needed to invest in two foundations, their people and their technology. They are currently on year three of the strategic plan and have incorporated ITIL training in the form of online, self-paced modules that align with budget and resource commitments. With leadership buy-in from the start, the IRS is on pace to complete their goals and are already seeing the benefits.

5.3 Leveraging the 299th Network Operations Security Squadron

The 299th NOSS is the Air National Guard NOSC. Their state-of-the-art facility affords a unique position to assist the Air Force with I-NOSC leadership transitions. For example, their facility has ample real-estate and qualified personnel to house a FAM course for new leadership personnel destined for one of the I-NOSCs. Such training of senior leadership at a central location would ensure continuity of service and standardization of operations. The personnel assigned to the 299th NOSS are perhaps the most experienced when it comes to the ITIL management process due to the minimal turn over rates associated with guard units.

Another opportunity is augmenting critical manning shortfalls. By understanding how the ANG NOSC works and the similarities within their leadership posture, the 299th NOSS may be able to augment IT management positions to support deployment taskings, exercises, or other situations.

5.4 624th Operations Center Personnel and the AOC Course

The 624th Operations Center (OC) receives direction from the 24th AF to execute command and control for AFNetOps. Indeed, cyber taskings for the Air Force are directed and coordinated from the 624th OC. The 624th OC is composed of a strategy, combat plans, combat operations and intelligence, surveillance, and reconnaissance divisions. Each division is responsible for shaping their functional area within the cyberspace construct as directed by US Cyber Command. The 624th OC assigns taskings similar to a traditional air operations center (AOC). The execution arm of this process are the I-NOSCs and functional areas within the ANG NOSC. Unlike traditional units taskings received from their respective AOC, cyberspace taskings are multi-layered and may involve coordination among multiple organizations outside of the chain of command. To help cyberspace operations align with tradition AOC processes, 624th OC personnel should be required to attend the AOC planning course at Hurlburt AFB.

5.5 Stagger Leadership

Permanent change of station moves are directly impacting the stability of the Air Force network posture. Identification of key positions should be accomplished to assist in future staffing requirements. Based on these inputs, staggering of leadership permanent change of station (PCS) orders should occur when possible. As an example, both the commander and director of operations for the 561st NOS will PCS during the summer of 2011, leaving of void of leadership experience. As an alternative, a civilian technical director or civilian deputy position should be examined to ensure continuity during leadership changeovers.

5.6 Standardized Network Monitoring Toolset

The AFNetOps squadrons have a responsibility to provide a service to their MAJCOM customers 24 hours a day, 7 days a week, 365 days a year. Their missions vary due to their geographic location and mission priorities; however, basic services

are common throughout the squadrons. The ability to employ a standardized network monitoring tolls set would enhance awareness, ensure continuity, and decrease spin-up time for personnel transferring amongst squadrons. Note, that during site visits each network operation squadron was observed using a unique monitoring interface with no standardization of metrics or measurements.

5.7 Tour Length

Due to the complexity associated with AFNetOps, tenure is important. In order to maintain a strong posture, stability is the foundation of success. In the AFNetOps community, an adversary may study a target for years to determine characteristics and weakness of a target. The lack of defined tour lengths creates an environment of high transfer rates, which results in constant training of new personnel and processes. To alleviate weaknesses associated with rapid turn overs, the positions should be a controlled four year tour. Additionally, essential positions should be coded as deployed-in-place or non-deployable.

Increase Active Duty Service Commitment (ADSC) for members attending specialized cyber training. In order for the AF to retain qualified personnel to defend their networks, an initiative to keep our professionals needs to be in place. There is a small community of A-Shred personnel that are tracked by AFSPC. Those personnel performing operational taskings in NetA and NetD capacities need to have their ADSC commitment adjusted accordingly. What the AF cannot continue doing is investing in their personnel and they spend one tour performing in that capacity then leave service for higher paying salaries. An increased ADSC retains those personnel for the time senior leadership determines and provides stability to our NetOps posture.

5.8 Test Suite

The Air Force should create and designate an organization (e.g., AFNIC) for evaluation of new processes, changes or maintenance tasks. Currently, there is no in-

herent and standardized unit that offers this capability to network operations squadrons. As a clearing house, the unit can ensure standardization across AFNetOps and identify observed issues that impact the entire enterprise. A reporting procedure would provide insight for the operational community to minimize risks. Note, the 346th Test Squadron performs operational testing, which is different from configuration evaluation.

More on the 346th TS: They operate and maintain the AF largest range infrastructure for Network Warfare Operations (NWOps) supporting Information Assurance (IA) testing, full spectrum NWOps testing and two deployable EMSEC test units. They have the AF's only Unified Capabilities range for testing capabilities and systems. NWOps ranges replicate NetA CITS infrastructure and AFNetOps three tiered architecture enabling the emulation of base IT infrastructure and computer system HW and SW. This test squadron is located near the 24th AF on Lackland AFB but they are functionally aligned under the 318th Information Operations Group within the 688th Information Operations Wing. This wing is also aligned under the 24th AF along with the 67th NWW. If resources and manpower were allocated, this could be a potential alternative.

299th NOSS is another potential location for a test suite. They currently house six suites of Air Force Bulwark Defender/SIMTEX Range Equipment. If used in tandem with the 246th TS, those units can share the load in working tasking orders as they are tasked out to the NetOps community.

5.9 Experience

An interesting observation during the site visits was a significant presence of new accessions. Although the individuals are highly motivated, at this point in their career they may present liabilities to the organization. As a paradigm to the flying world, seasoned pilots are sought for flight test instructors and stan eval sections. The primary challenge to overcome is recognition by AFPC that assigning accessions to these positions is detrimental to the organization and the individual. As an alterna-

tive, personnel assigned to an I-NOSC should have at least one tour at a base level squadron or equivalent to help gain an understanding and appreciation of the mission set.

5.10 Service Portfolio

To improve ITIL awareness, the 24th AF should create and manage a service portfolio to quantify the services that are provided to the users. Customer orientation is key to ITIL, however, the services offered and, more importantly, the priority of those services is nonexistent. A service portfolio identifies services and the impact to an organization's mission if the services are degraded or lost. Past, current and future planned services are contained within the service portfolio and should be the core document for ITIL assessment and organization. Additionally, the service portfolio should detail the responsible parties in reference to service and operational level agreements. This notion will help determine areas of responsibilities and provides a notion of critical roles from an enterprise perspective.

5.11 Continuity of Operations

Currently, there is no fail over capability for the 561st or the 83rd NOS. Namely, there is continuity of operations (COOP) plan in the event of a catastrophic cascading failure. Now more than ever, the ability to recover and be resilient through an attack is critical. A vital aspect of this recommendation is the reliance on standardized of AFNetOps. A standard infrastructure, service and operations will enable the ability to quickly and efficiently transition to a fail over system in the event of an emergency.

5.12 Embed a Subject Matter Expert (SME) at 624th OC

A SNCO SME needs embedded on the 624th OC staff. Having come from 83rd or the 561st NOS as a follow on the SME would be seasoned and able to articulate issues with tasking orders directed to the NetOps squadrons. The SME will be seasoned with years of NetOps experience and will be able to head off challenges prior to release.

The SME will be an important component advocating the NOS perspective at the 624th OC level (see Figure 15).

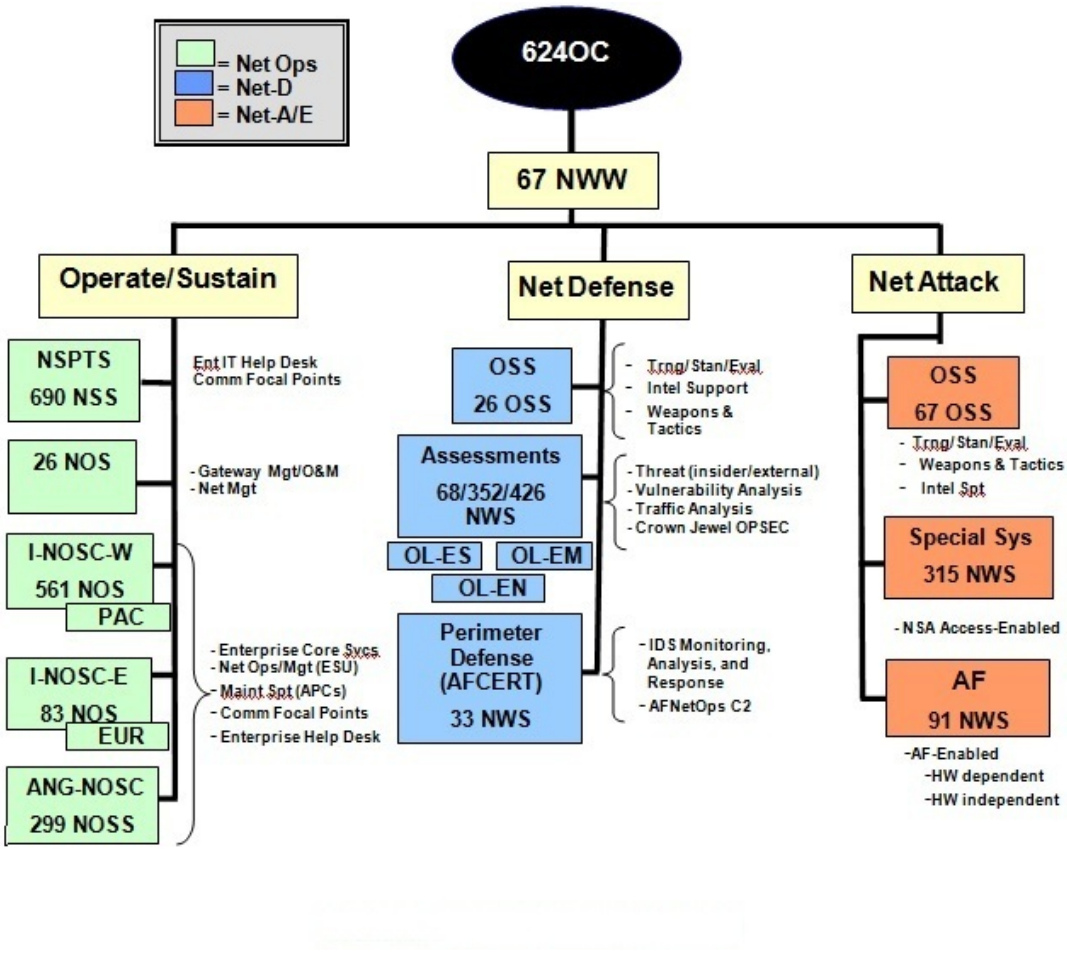

Figure 15: AFNetOps Execution Elements

VI. Summary & Conclusion

6.1 Summary

Over the past seven years, there were pockets of ITIL/ITSM trials on USAF facilities. Through continual self improvement, ITIL hos dramatically improved upon since its inception. The Air Force has undergone a serious transformation towards NetOps and the implications will be felt from this transformation for decades to come. As AF NetOps continues to evolve, the Continual Self Improvement component of ITSM changes with it to meet mission specifications.

Industry provided a few lessons that the AF can learn from. Microsoft and AT&T went through massive budget cuts that drove them to ITIL [25]. Recently, IBM incorporated ITIL concepts into their IBM Tivoli Service Request Manager and received the Gold Level ITIL v3 Certification which is the highest possible ITIL certification in three different categories: Incident Management, Change Management and Request Fulfillment Management [8]. The AF has undergone similar cuts through various reduction in force and force management programs. A portion of those savings should be diverted towards an education initiative for leadership to fully understand what ITIL will bring to the IT force and to tenured personnel with ITIL focused initiatives.

Case studies have been performed on a government agency in France to change from face-to-face to online services. Of all the areas affected, service support (Operations) were constantly in a "fire-fighting" reactive mode during the study. Another issue was that the contact for support and service desk and incident management were not functioning properly per the SLA. Problem, change and configuration management also suffered greatly during this study [26]. Lessons such as these are invaluable for the USAF to properly model our services appropriately to avoid similar pitfalls.

The I-NOSC functions within the 83rd, 561st NOS and 299th NOSS are working at an incredible pace 24/7/365. Each entity have their own unique challenge to deal with while maintaining C2 and defending the network. Current efforts to thwart intrusions at their level have been effective given that attack measures are changing

by the minute. The plan to migrate toward a centralized control centralized execution was the right decision given the state of how our networks were being managed. The ITIL process is the right mechanism the AF needs in order to streamline our processes and provide better customer service to the end user.

6.2 Conclusion

The full inclusion of NOS operations into the ITSM process is what the AF needs to adopt. Initial steps have been taken however, there is substantial work to be accomplished. There are a few areas that need to be accomplished before the AF will benefit from the ITIL process:

1. Corporate leadership buy in
2. Investment in personnel
3. Educating cyber professionals early and bi-annually through ADLS
4. Stability within the organization

It would be prudent for the Air Force to take a more aggressive stance towards incorporating ITIL. This process has been around for 30 years and have been constantly updated for the better through continual self improvement. Positive work have been accomplished through collaborative efforts authoring TO 00-33A-1100 which outlines guidance for the AFNet Operational Change Management Process. The TO applies to all cyber career fields as well as any other Air Force Specialty Code technicians working on the AFNet. Additionally, the practices and procedures within the TO were built around ITIL. This TO is in draft however, the three organizations responsible for its creation are working together to ensure accuracy for day to day ops.

Several independent studies have identified that over 80 percent of IT system downtime is due to people and processes, not technology [20]. The units all have a unique perspective on how ITIL is incorporated into their organizations. One point of view considers themselves as the ITIL Center of Excellence for the Air Force. They

are working on molding ITIL into operational needs for the Air Force and the Theory of ITIL practices. Another vision perceives themselves as leading AFNet effort for the Air Force. The third envisions themselves as having the most mature ITIL processes in all of AFNetOps. Three squadrons, three different perspectives, one vision towards standardization and flawless customer service.

The NetOps squadrons first priority is meeting customers requirements. Each squadron have sections specializing in ITIL/ITSM and are taking necessary measures to merge it fully into I-NOSC operations. This begins with corporate buy-in. Before leadership can make decisions on ITSM governance, they must be educated on the implications of not taking this path to optimal service management. This research found that the leaders of these organizations have been educated and are acting on the management of their squadrons using this principle. The commanders are doing everything they can do to maintain C2 at the MAJCOMs they are responsible for via ITSM processes. The other functional areas of ITIL that are controlled and operated at the strategic levels are Service Strategy and Service Design. Educating leadership at those levels will benefit the IT community as a whole. Once that is accomplished, the corporate buy-in component will be able to leverage resources across the Five Year Defense Plan and allocate them accordingly to further strengthen our NetOps footprint within the AF-GIG.

An investment in personnel has been accomplished at each of the squadrons this research is focused on. The issue the AF as a whole is experiencing is retaining those trained personnel. Corporate America have been the beneficiary of military trained IT specialists for years and this continues today with our NetOps trained personnel. With the exception of the 299th NOSS, the other squadrons have personnel transitioning in, receiving training and upon finishing up their service commitment, leave service. The AF cannot survive the Cyber-Storm on the horizon and AFNetOps will never flourish as intended. Indeed, It starts and ends with education but there needs to some sort of service commitment for specialized trained personnel within the squadrons. If we shift the paradigm slightly and commit the 17DXA and 1B4 that are performing NetA

and NetD functions on the network, a 6 year commitment is reasonable. This will serve as the return on investment for the specialized training they received. If this will not suffice, a bonus of some sort should be considered to keep these professionals in service until they reach the 10 year mark.

Professionals visited displayed a keen knowledge base in their functional areas. A few of the military personnel were not fully versed on the ITIL/ITSM principles but knew the processes are invaluable to the organization. Educating of these personnel early is crucial to having ingrained knowledge of ITIL foundation follow them throughout their career. The incorporation of TO 00-33A-1100 and full release of Remedy 7.1 will benefit the squadrons greatly. Components of Remedy 7.1 will ease the day to day tension of the NetOps squadron in all facets of ITSM. In essence, the relationship between the 624th OC and the NOS units executing the orders stand to benefit from these initiatives.

The NetOps squadrons are being hampered by many things but most importantly fluid personnel. Personnel in these crucial points of presence for for NetOps are not functionally in the seat long enough to have a real impact on operations. Deployments, mid-tour classes to INWT or new accessions are putting the organizations at risk. This applies to the 83rd and 561st NetOps squadrons. Due to the nature of their business, these organizations are not the place for those individuals. For AFPC to send these personnel to the NetOps squadrons for OJT signifies the wrong picture and threatens AFNetOps as a whole. This is why there needs to be leadership buy-in with the understanding that this is no place for first duty assignments of ANY Cyber personnel. Both squadrons are the beneficiary of new accessions and that component of our AFNetOps posture is our weak link.

These areas were the discoveries that stood out over this research. Detailed analysis reside within the chapters of this GRP but the areas listed are what needs attention right now. Organizations tend to invest in what they deem is important to them. If Cyber is as important to the AF as we say it is, a substantial investment

needs to be directed towards it in order for the USAF to Fly, Fight and Win in Air, Space and Cyberspace.

6.3 Future Research

1. Air Force Network Integration Center become testing facility for maintenance orders (TCNO, NTO, TCTO's) prior to distribution to I-NOSCs.
2. Fail-over research between the I-NOSCs. What are the limiting factors?

Bibliography

1. Tom Oliphant, "ITIL V3 Service Lifecycle 561st NOS," 2011.
2. Tom Oliphant, "ITIL V3 Service Lifecycle 561st (2) NOS," 2011.
3. Instruction, A.F., "TO 00-33A-1100 Draft Organizational Change Management," 2011.
4. Instruction, A.F., "Air Force Network Operations Implementation Plan AFNetOps (Draft)," 2006.
5. Valerie Arraj, "ITIL: The Basics," 2010. http://www.best-management-practice.com/gempdf/ITIL_The_Basics.pdf/.
6. Kate Winter, "Disneys ITILJourney," 2010. http://www.best-management-practice.com/gempdf/disney_itil_journey.pdf publisher=TSO.
7. Scott Fontaine, "New USAF Cyber Unit Grapples With Data Overload," 2010. http://www.defensenews.com/story.php?i=5043141/ publisher=Defense News.
8. IBM Software, "IBM Solution Receives Highest Possible ITIL Certification," 2009. http://www-01.ibm.com/software/tivoli/governance/action/12032009.html/.
9. Angela Steel, "Taking IT out of the corner, Mller Dairy," 2011. http://www.corp.att.com/consulting/it-transformation/ publisher=APM Group.
10. Maggie Kneller, "Executive Briefing: The Benefits of ITIL," 2010. http://www.best-management-practice.com/gempdf/OGC_Executive_Briefing_Benefits_of_ITIL.pdf/ publisher=The Stationary Office.
11. B. Potgieter, J. Botha, and C. Lew, "Evidence that use of the itil framework is effective," in *18th Annual conference of the national advisory committee on computing qualifications, Tauranga, NZ*, Citeseer, 2005.
12. Alison Cartlidge, "An Introductory Overview of ITIL V3," 2007. http://www.best-management-practice.com/gempdf/itSMF_An_Introductory_Overview_of_ITIL_V3.pdf/.
13. Lt Col Eric P. Delange, "83 Network Operations Squadron Mission Brief," 2010.
14. Capt. David A. Lavine, "Integrated Network Operations and Security Center Brief," 2006.
15. 184th Intelligence Wing, "184th Intelligence Wing Units," 2011. http://www.184iw.ang.af.mil/units/index.asp/ publisher=KANG Fighting Jayhawks.

16. Michael Kerver, "Air Force officials make first major move toward a central network," 2009. http://www.af.mil/news/story.asp?id=123178188/ publisher=Air Force Network Integration Center.

17. U. DoD, "Jp1-02: Department of defense dictionary of military and associated terms," 2010.

18. U. DoD, "Air force doctrine document 1-2," 2007.

19. W. Lynn III, "Defending a new domain: The pentagon's cyberstrategy," tech. rep., Office of the Deputy Secretary of Defense Washington DC, 2010.

20. Nick Mossing, "Air Combat Command shares transformation success stories, Network Operations and Security Center," *Intercom, Journal of the Air Force C4ISR community* , p. 13, 2004.

21. Instruction, A.F., "33-115 Volume 1: Network Operations (NetOps)," 2006.

22. Instruction, A.F., "Integrated Network Opearations & Security Center (I-NOSC) Implementation Plan (Draft)," 2006.

23. Instruction, A.F., "Air Force Network Operations Enterprise Service Unit Implementation Plan," 2006.

24. APM Group, "Using ITIL at the IRS: A business journey," 2011. http://www.best-management-practice.com/gempdf/Using_ITIL_at_the_IRS_Case_Study_Jan_11.pdf/.

25. AT&T Enterprise, "IT Transformation," 2011. http://www.corp.att.com/consulting/it-transformation/.

26. Rachid Meziani, Imad Saleh, "e-government: ITIL-based service management case study," 2010. http://portal.acm.org/citation.cfm?id=1967565/ publisher=ACM.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From – To)*
16-06-2011	**Graduate Research Project**	18 June 2010- 16 June 2011

4. TITLE AND SUBTITLE

Leveraging ITIL/ITSM into Network Operations

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)

Davis A. Lavine Sr., Maj, USAF

5d. PROJECT NUMBER
N/A

5e. TASK NUMBER
N/A

5f. WORK UNIT NUMBER
N/A

7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S)
Air Force Institute of Technology
Graduate school of Engineering and Management
2950 Hobson Way
WPAFB OH 45433-7765

8. PERFORMING ORGANIZATION REPORT NUMBER

AFIT/ICW/ENG/11-07

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Air Force Space Command, 561st Network Operations Squadron
Attn: Maj. Paul Williams
Paul.williams.3@us.af.mil DSN 692-9338
561 Network Operations Squadron
Peterson AFB, CO 80914

10. SPONSOR/MONITOR'S ACRONYM(S)
ITIL/ AFNetOps/MAJCOM/ I-NOSC

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
N/A

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approval for public release; distribution unlimited. This material is declared a work of the U. S. Government and is not subject to copyright protection in the United States.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Air Force Network Operations (AFNetOps) controls the AF portion of the Global Information Grid (GIG). In order to do this efficiently, the USAF had to change the way it was operating and go away Centralized Control. Decentralized execution towards Centralized Control, Centralized Execution. This was done largely in part because the USAF was struggling in protection of critical information and the networks interconnection all of our installations. In the late 80's the United Kingdom created Information Technology Infrastructure Library (ITIL) whose purpose is to provide a practical no- nonsense framework for identifying, planning, delivering and supporting IT services for a business. Over the years, ITIL has become the defacto standard for all IT Service Management. In consolidating our Network Operations and Security Center operations, the USAF decided to take steps towards incorporating this standard. This research discovered how well ITSM was integrated into our AFNetOps posture and the collaborative efforts to standardize change management for the benefit of the Air Force. If indeed the USAF is to become another ITIL success story, it resides with the IT Service Management framework of guiding our NetOps.

15. SUBJECT TERMS
ITIL, ITSM, AFNetOps, I-NOSC

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
REPORT	**ABSTRACT**	**c. THIS PAGE**			**Dr Robert F Mills**
U	**U**	**U**	**UU**	61	**19b. TELEPHONE NUMBER** *(Include area code)* 937-255-3636 ext 4527

Standard Form 298 (Rev: 8-98)
Prescribed by ANSI Std. Z39-18